Notice of Allowability	Application No.	Applicant(s)	
	10/029,765	O'DONNELL ET AL.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *3/31/06*.

2. ☒ The allowed claim(s) is/are *1-51 and 54-62*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20060607* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Robin Reasoner on 6/7/2006.

Please amend the claims as follows:

1. (Currently Amended) A computer-implemented method for managing temporary access to a first user's data, comprising:

receiving, from a first user, a message at an authentication server, the first user having an authentication credential with respect to a first user's account used to interact with the first user's data through an application, the message that a second user be granted temporary access to the first user's data through the application;

receiving, from the second user, a request at the authentication server, the request to access the first user's data through the application; and

responsive to the request from the second user, obtaining the first user's authentication credential from the authentication server and granting the second user temporary access to the first user's data through the application by providing to the application the first user's authentication credential, wherein the first user's authentication credential is not provided to the second user.

2. (Previously presented) The method of claim 1, wherein granting the second user temporary access comprises activating a temporary access credential for the second user.

3. (Previously presented) The method of claim 1, wherein granting the second user temporary access comprises creating an entity relationship between an account associated with the second user and an account associated with the first user.

4. (Original) The method of claim 3, wherein the account associated with the second user comprises a support representative account.

5. (Previously presented) The method of claim 1, wherein the message identifies the second user and specifies a level of access for the second user, and wherein granting the second user temporary access comprises granting the specified level of access.

6. (Original) The method of claim 1, wherein the second user belongs to a group of users, and the message identifies the group of users to which the second user belongs.

7. (Original) The method of claim 6, further comprising:

receiving an identifier from the second user, identifying the second user as belonging to the group of users.

8. (Original) The method of claim 6, further comprising:

authenticating the second user as belonging to the group of users.

9. (Original) The method of claim 6, wherein the group comprises support representatives.

10. (Previously presented) The method of claim 1, further comprising:

authenticating the second user;

and wherein granting the second user temporary access to the first user's data comprises:

responsive to the request from the second user and responsive to the authentication of the second user being successful, granting the second user temporary access to the first user's data by providing the first user's authentication credential.

11. (Previously presented) The method of claim 1, wherein granting the second user temporary access to the first user's data comprises granting the second user a level of access different from a level of access available to the first user.

12. (Original) The method of claim 1, wherein receiving the message comprises receiving the message via a network.

13. (Original) The method of claim 12, wherein receiving the request comprises receiving the request via the network.

14. (Original) The method of claim 12, wherein receiving the request comprises receiving the request via a second network.

15. (Previously presented) The method of claim 1, further comprising storing in an audit log information describing the second user's access to the first user's data and identifying the second user in connection with the access.

16. (Currently Amended) A computer-implemented method for managing levels of access to a first user's data for at least two users, comprising:

establishing a control relationship between a first user's authentication credential and a second user's authentication credential, the control relationship allowing the first user to specify at least one parameter of the second user's level of access to a first user's data;

receiving, from a first user, a message at an authentication server, the first user having an authentication credential with respect to a first user's account used to interact with the first user's data through an

application, the message that a second user be granted temporary access to the first user's data through the application;

receiving, from the second user, a request at the authentication server, the request to access the first user's data through the application; and

responsive to the request from the second user, granting the second user access to the first user's data through the application according to the second user's level of access as specified by the first user, by providing to the application the first user's authentication credential, wherein the first user's authentication credential is obtained from the authentication server and is not provided to the second user.

17. (Original) The method of claim 16, wherein the second user is a support representative.

18. (Previously presented) The method of claim 16, further comprising:

terminating the second user's access to the first user's data.

19. (Previously presented) The method of claim 1 or 16, further comprising:

terminating the second user's access to the first user's data after a predetermined time period.

20. (Original) The method of claim 19, wherein the predetermined time period is selectable by the first user.

21. (Previously presented) The method of claim 1 or 16, further comprising:

terminating the second user's access to the first user's data after the second user has accessed the first user's data a predetermined number of times.

22. (Original) The method of claim 21, wherein the predetermined number of times is selectable by the first user.

23. (Previously presented) The method of claim 1 or 16, further comprising:
terminating the second user's access to the first user's data in response to a command received from the first user.

24. (Previously presented) The method of claim 1 or 16, further comprising:
terminating the second user's access to the first user's data in response to a predetermined event.

25. (Previously presented) The method of claim 1 or 16, further comprising:
responsive to granting the second user access, outputting, to the first user, notification of the second user's access to the first user's data.

26. (Previously presented) The method of claim 1 or 16, further comprising:
responsive to granting the second user access, storing information describing the second user's access to the first user's data.

27. (Original) The method of claim 26, wherein storing information comprises storing the information in an audit log.

28. (Previously presented) The method of claim 1 or 16, further comprising:

storing information describing at least one subsequent interaction with the first user's data.

29. (Previously presented) The method of claim 28, wherein storing information comprises, for each interaction, storing information identifying which user accesses the first user's data.

30. (Previously presented) The method of claim 1 or 16, wherein the access to the first user's data by the second user is masked so that an application through which the second user accesses the first user's data is unable to distinguish the access by the second user from access by the first user.

31. (Original) The method of claim 16, wherein the first user's level of access is different from the second user's level of access.

32. (Previously presented) The method of claim 1 or 16, wherein the first user's data comprises at least one selected from the group consisting of:

a data file;

a data file stored at a server; and

data associated with the first user.

33. (Original) The method of claim 1 or 16, wherein the steps of the method are performed by a web-based application.

34. (Currently Amended) A system for granting to a second user access to a first user's data in response to a message from a first user, comprising:

an authenticator communicatively adapted to receive over a network connection authentication credentials of the first and second users and adapted to authenticate each user from the authentication credentials;

an access level control module, communicatively coupled to the authenticator, for defining for each user a level of access to a first user's data; and

a resource interface, communicatively coupled to the access level control module, for granting the second user access to the first user's data through the resource interface by providing the first user's authentication credential to the authenticator for authentication, wherein the first user's authentication credential is obtained from an authentication server and is not provided to the second user.

35. (Original) The system of claim 34, wherein the access level control module activates a temporary access credential for the second user.

36. (Original) The system of claim 34, wherein the access level control module creates an entity relationship between an account associated with the second user and an account associated with the first user.

37. (Currently Amended) A system for granting to a second user access to a first user's data in response to a message from a first user, comprising:

an access level control module, for establishing a control relationship between an authentication credential associated with the first user and an authentication credential associated with the second user, the control relationship allowing the first user to control at least one parameter of the second user's level of access; and

a resource interface, coupled to the access level control module, for granting the second user access to the first user's data through the resource interface according to the second user's level of access, by providing the first user's authentication credential to an authenticator, wherein the first user's authentication credential is obtained from an authentication server and is not provided to the second user.

38. (Previously presented) The system of claim 34 or 37, wherein the resource interface further terminates the second user's access to the first user's data.

39. (Previously presented) The system of claim 34 or 37, wherein the resource interface further terminates the second user's access to the first user's data after a predetermined time period.

40. (Original) The system of claim 39, wherein the predetermined time period is selectable by the first user.

41. (Previously presented) The system of claim 34 or 37, wherein the resource interface further terminates the second user's access to the first user's data after the second user has accessed the first user's data a predetermined number of times.

42. (Original) The system of claim 41, wherein the predetermined number of times is selectable by the first user.

43. (Previously presented) The system of claim 34 or 37, wherein the resource interface further terminates the second user's access to the first user's data in response to a command received from the first user.

44. (Previously presented) The system of claim 34 or 37, wherein the resource interface further terminates the second user's access to the first user's data in response to a predetermined event.

45. (Previously presented) The system of claim 34 or 37, further comprising:

an output device, coupled to the resource interface, for outputting, to the first user, notification of the second user's access to the first user's data.

46. (Previously presented) The system of claim 34 or 37, further comprising:

a storage device, coupled to the resource interface, for storing information describing the second user's access to the first user's data.

47. (Previously presented) The system of claim 46, wherein the storage device stores information identifying which user accesses the first user's data.

48. (Previously presented) The system of claim 34 or 37, wherein the access to the first user's data by the second user is masked so that an application through which the second user accesses the first user's data is unable to distinguish the access by the second user from access by the first user.

49. (Previously presented) The system of claim 34 or 37, wherein the first user's data comprises at least one selected from the group consisting of:

a data file;

a data file stored at a server; and

data associated with the first user.

50. (Currently Amended) In a client/server system for granting to a second user access to a first user's data in response to a message from a first user specifying that the second user be granted access to the first user's data, a server comprising:

an authenticator, for authenticating each user according to authentication credentials;

an access level control module, coupled to the authenticator, for defining a level of access to the first user's data for each user; and

a resource interface, coupled to the access level control module, for granting to a client operated by the second user access to the first user's data through the resource interface by providing the first user's authentication credential to the authenticator, wherein the first user's authentication credential is obtained from an authentication server and is not provided to the second user.

51. (Currently Amended) In a client/server system for granting to a second user access to a first user's data in response to a message from a first user specifying that the second user be granted access to the first user's data, a server comprising:

an access level control module, for establishing a control relationship between the first user's authentication credential and the second user's authentication credential, the control relationship allowing the first user to control at least one parameter of the second user's level of access; and

a resource interface, coupled to the access level control module, for granting to the client operated by the second user access to the first user's data through the resource interface according to the second user's level of

access, by providing the first user's authentication credential to ~~the~~ an authenticator, wherein the first user's authentication credential is obtained from an authentication server and is not provided to the second user.

52. (Cancelled)

53. (Cancelled)

54. (Currently Amended) A computer program product comprising a computer-usable medium having computer-readable code embodied therein for managing temporary access to a first user's data, comprising:

computer-readable program code configured to cause a computer to receive a message at an authentication server from a first user, the first user having an authentication credential with respect to the first user's data, the message that a second user be granted temporary access to the first user's data;

computer-readable program code configured to cause a computer to receive a request at the authentication server from the second user, the request to access the first user's data; and

computer-readable program code configured to cause a computer to, responsive to the request from the second user, obtain the first user's authentication credential and grant the second user temporary access to the first user's data by providing the first user's authentication credential to an authenticator, wherein the first user's authentication

credential is obtained from the authentication server and is not provided to the second user.

55. (Original) The computer program product of claim 54, wherein the computer-readable program code configured to cause a computer to grant the second user access comprises computer-readable program code configured to cause a computer to activate a temporary access credential for the second user.

56. (Original) The computer program product of claim 54, wherein the computer-readable program code configured to cause a computer to grant the second user access comprises computer-readable program code configured to cause a computer to create an entity relationship between an account associated with the second user and an account associated with the first user.

57. (Previously presented) The computer program product of claim 54, further comprising:

computer-readable program code configured to cause a computer to authenticate the second user;

and wherein the computer-readable program code configured to cause a computer to grant the second user access to the first user's data comprises:

computer-readable program code configured to cause a computer to, responsive to the request from the second user and responsive to the authentication of the second user being successful, grant the second user access to the first user's data by providing the first user's authentication credential.

58. (Currently Amended) A computer-implemented computer program product for managing levels of access to a first user's data for at least two users, comprising:

computer-readable program code configured to cause a computer to establish a control relationship between a first user's authentication credential and a second user's authentication credential, the control relationship allowing the first user to specify at least one parameter of the second user's level of access to a first user's data;

computer-readable program code configured to cause a computer to receive, from a first user, a message at an authentication server, the first user having an authentication credential with respect to a first user's account used to interact with the first user's data through an application, the message that a second user be granted temporary access to the first user's data through the application;

computer-readable program code configured to cause a computer to receive, from the second user, a request at ~~an~~ the authentication server the request to access the first user's data through the application; and

computer-readable program code configured to cause a computer to, responsive to the request from the second user, grant the second user access to the first user's data through the application according to the second user's level of access as specified by the first user, by providing to the application the first user's authentication credential, wherein the first user's authentication credential is obtained from the authentication server and is not provided to the second user.

59. (Previously presented) The computer program product of claim 54 or 58, further comprising:

computer-readable program code configured to cause a computer to, responsive to granting the second user access, store information describing the second user's access to the first user's data.

60. (Previously presented) The computer program product of claim 54 or 58, further comprising:

computer-readable program code configured to cause a computer to store information describing at least one subsequent interaction with the first user's data.

61. (Previously presented) The computer program product of claim 60, wherein the computer-readable program code configured to cause a computer to store information comprises, computer-readable program code configured to cause a computer to, for each interaction, store information identifying which user accesses the first user's data.

62. (Previously presented) The computer program product of claim 54 or 58, wherein the access to the first user's data by the second user is masked so that an application through which the second user accesses the first user's data is unable to distinguish the access by the second user from access by the first user.

Allowable Subject Matter

Claims 1-51 and 54-62 are allowed. The following is an examiner's statement of reasons for allowance:

The closest prior art previously cited, namely Brickell, Chow, Onishi, Sudia, Control-F1, and Zhang teach various authentication systems for delegation of user rights and/or access to data. However, none of the prior art teaches granting a second user access to a first user's data by obtaining the first user's authentication credential from the authentication server and sending this first user's authentication credential to the application/authenticator for access to the data, without the first user's authentication credential being provided to the second user.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffrey D Popham
Examiner
Art Unit 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER